Report to The President's Council on Integrity and Efficiency

Federal Agencies' Controls over the Access, Disclosure and use of Social Security Numbers by External Entities

Social Security Administration
Office of the Inspector General
February 2003

Introduction

Objective

Our objective was to provide the President's Council on Integrity and Efficiency (PCIE) with an assessment of Federal agencies' controls over the access, disclosure and use of Social Security numbers (SSN) by external entities.

Background

The SSN was created in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. However, over the years, the SSN has become a de facto national identifier used by Federal agencies, State and local governments, and private organizations. While a number of laws and regulations require the use of SSNs for various Federal programs, they generally impose limitations on how these SSNs may be used.

Although no single Federal law regulates the overall use and disclosure of SSNs by Federal agencies, the Freedom of Information Act of 1966, the Privacy Act of 1974, and the Social Security Act Amendments of 1990 generally govern disclosure and use of SSNs (Appendix A). In addition, a number of Federal laws lay out a framework for Federal agencies to follow when they establish information security programs that protect sensitive personal information, such as SSNs.[1]

The expanded use of the SSN as a national identifier provides a tempting motive for many unscrupulous individuals to acquire an SSN and use it for illegal purposes. While no one can fully prevent SSN misuse, Federal agencies have some responsibility to limit the risk of unauthorized disclosure of SSN information. Because of concerns related to perceived widespread sharing of personal information and occurrences of identity theft, congressional requesters asked the General Accounting Office (GAO) to study how, and to what extent, Federal, State and local government agencies use individuals' SSNs and how these entities safeguard records or documents containing those SSNs.[2] The information the

[1] *The Government Information Security Reform provisions of the Fiscal Year 2001 Defense Authorization Act, Pub. L. No. 106-398, Subtitle G (2000); the Clinger-Cohen Act of 1996, Pub. L. No. 104-106, Division D and E (1996); the Paperwork Reduction Act of 1995, Pub. L. No. 104-13 (1995); the Computer Security Act of 1987, Pub. L. No. 100-235 (1988). See also Office of Management and Budget guidance, such as Circular A-130.*

[2] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

agencies provided was self-reported, and GAO did not verify the responses.

The Chairman of the Subcommittee on Social Security, House Ways and Means Committee, requested that the Social Security Administration's Office of the Inspector General (OIG) look at the way Federal agencies disseminate and control the use of SSNs. After consultation with the PCIE, we agreed to serve as audit lead for 15 participating OIGs (Appendix B) and prepare the final report. As part of our review, we coordinated with GAO to avoid duplication of effort. This report serves as a follow-up to GAO's study and provides a more in-depth analysis of Federal agencies' SSN controls related to contractor access, databases, non-Government access, and disclosure.

Most OIGs either have issued or will be issuing individual reports to their respective departments or agencies. The individual OIG reports make recommendations for corrective actions at the department or agency level.

Scope and Methodology

To accomplish the objective, OIGs

- reviewed controls over the use and protection of SSNs within their respective agency;
- interviewed agency personnel responsible for controls over the access, disclosure and use of SSNs;
- reviewed relevant agency procedures and practices;
- reviewed applicable laws and regulations;
- observed selected contractor activities; and
- reviewed relevant agency audit reports.

Each OIG focused its work on one program within its respective agency.[3] As such, the findings in this report should not be extrapolated to all programs within each agency. See Appendix C for the specific agency program each OIG reviewed.

[3] The Department of Defense assessed SSN controls for three programs.

Results of Review

Despite Federal agencies' safeguards to prevent improper access, disclosure and use of SSNs by external entities, agencies remained at-risk to such activity. Of the 15 agencies reviewed,

- 14 lacked adequate controls over contractors' access to and use of SSNs,
- 9 had inadequate controls over access to SSNs maintained in their computer systems,
- 2 did not have adequate controls over non-Government and/or non-contractor entities' access to and use of SSNs, and
- 1 did not make legal and informed SSN disclosures.

Federal Agencies Placed Safeguard Requirements on Contractors But Lacked Adequate SSN Controls

Federal agencies often use contractors to assist them in carrying out their statutory responsibilities. These contracts often contain standard language related to safeguarding personal information. Contracts may also contain penalty provisions for contractor misuse of information. Federal agencies incorporate different practices to ensure they have appropriate controls over contractor access to and use of SSNs. These include, but are not limited to, passwords and computer identifications; access to information on a need to know basis; periodic review of current computer users; staff and contractor confidentiality agreements; security awareness training; and secure work areas.

Although Federal agencies generally placed these safeguard requirements on contractors, 14 (93 percent) of 15 OIGs reported inadequate controls over contractors' access to and use of SSNs. For example, eight agencies had not performed site inspections to ensure contractors had upheld their obligation to protect the confidentiality and security of SSNs. One agency, which performed on-site inspections, did not adequately address the security of personal identifying information, such as SSNs. Moreover, two OIGs raised concerns about controls over contractors' security practices for file storage; one noted instances in which contractors maintained personal identifying information in unlocked file cabinets or storage rooms, and another noted that several agency

contractors left sensitive records on desktops or open shelves after normal working hours.

Two OIGs also reported problems regarding contractors' access to Federal agencies' databases. For example, these OIGs identified instances in which their agencies granted system access to contractors before they completed background security investigations. Additionally, one agency lacked adequate controls for deleting contractors' system access after they left the agency. Moreover, one agency did not have a process in place that systematically identified contractors who had access to sensitive information.

Two OIGs also identified instances in which agency contracts lacked the Privacy Act notice or the agency had no contract at all. For example, 1 agency had omitted the Privacy Act clause in 11 of 16 contracts. Another OIG noted instances in which contractors had access to personal data, although no Memorandum of Understanding existed between the agency and the contractor. Appendix C identifies the OIGs that reported their respective agencies had inadequate controls over contractors' access to and use of SSNs.

Federal Agencies Placed Controls over Access to Individuals' SSNs Maintained in Their Databases, But Weaknesses Existed

Federal agencies that allowed access to their databases generally had standard information security controls in place. Agency controls included, but were not limited to, security clearances before granting computer access, computer access controlled by job title, unique user identification and passwords, firewalls, encrypted data transportation, intrusion detection systems, and physical access controls. In addition, some agencies emphasized the users' responsibility to safeguard data through written agreements and computer screen Privacy Act notices. Although agencies limited access to their databases primarily to employees, most agencies also authorized systems access to external entities for specific purposes. For example, some agencies allowed other agencies access to their databases to assist in beneficiary eligibility determinations and provide such services as software design and support and data processing.

Despite Federal agencies' safeguards, 9 (60 percent) of 15 OIGs reported their respective agencies had inadequate controls over access to SSNs maintained in their databases. For example, one

agency granted systems access to its employees before completing background security checks while others were not monitoring user access to ensure users were still current employees or contractors. Other identified weaknesses included physical access controls, implementation and monitoring of technical security configuration standards and monitoring security violations. Because of the sensitive nature of information security issues, we chose to withhold detailed descriptions of information security control weaknesses identified by OIGs. Appendix C identifies the OIGs that reported their respective agencies had inadequate controls over access to SSNs maintained in their databases.

Federal Agencies Generally Had Adequate Controls over Non-Government/Non-Contractor Entities' Access to and Use of SSNs

Federal agencies generally granted access to and use of SSNs to those entities whose requests fell under the Freedom of Information or Privacy Act exclusions. Two OIGs reported their agencies also granted life insurance and/or pension companies access to deceased individuals' SSNs.[4] However, about half of the OIGs reported their respective agencies did not grant non-Government and/or non-contractor entities' access to and use of SSNs.

Two (13 percent) of 15 OIGs reported their agencies did not have adequate controls over non-Government/non-contractor entities' access to and use of SSNs. One OIG reported its agency had no standard contract language to include privacy act safeguards. Another OIG reported its agency did not establish financial standards for outside parties to meet prior to gaining access to data containing SSN information. Appendix C identifies the OIGs that reported their respective agencies had inadequate controls over non-Government and/or non-contractor entities' access to and use of SSNs.

Federal Agencies Generally Made Legal and Informed Disclosures of SSNs to External Entities

One (7 percent) of 15 OIGs reported its agency did not make legal and informed SSN disclosures. This OIG identified instances in which the agency did not inform research study participants that providing their SSNs was voluntary. The remaining OIGs reported their respective agencies generally made legal and informed SSN

[4] The Privacy Act does not apply to deceased individuals.

disclosure to external entities.[5] In doing so, agencies included Privacy Act notices on forms and had matching agreements with other entities that outlined the agencies' roles in protecting personal identifying information. Federal agencies also informed individuals when they needed to provide their SSN to apply for benefits, by what legal authority they were requesting the SSN, and how the agency was going to use the SSN. Federal agencies disclosed individuals' SSNs to various external entities, including Federal and State agencies, insurance companies, universities and researchers.

Although the 14 remaining OIGs reported their agencies generally made legal and informed SSN disclosures, they identified instances in which agency practices increased the risk external entities may have improperly obtained and misused SSNs. For example, one OIG identified instances in which its agency unnecessarily displayed SSNs on documents it sent to external entities that may not have had a need to know. Another OIG identified instances in which its agency inadvertently omitted the Privacy Act notice on one of its forms, and another OIG identified instances in which its agency provided SSNs to another agency in error. Appendix C identifies the OIG that reported its agency made improper disclosures of SSNs to external entities.

[5] For purposes of this report, we consider SSN disclosure to have occurred when an agency provides an SSN to an external entity that did not already have it.

Conclusion

Some Federal agencies are at-risk for improper access, disclosure and use of SSNs by external entities, despite safeguards to prevent such activity. We recognize Federal agencies' efforts cannot eliminate the potential that unscrupulous individuals may inappropriately acquire and misuse SSNs. Nonetheless, we believe each Federal agency has a duty to safeguard the integrity of SSNs by reducing opportunities for external entities to improperly obtain and misuse the SSNs. Given the potential risk for individuals to engage in such activity, we believe Federal agencies would benefit by strengthening some of their controls over the access, disclosure and use of SSNs by external entities.

Appendix A

Federal Laws that Restrict Disclosure of the Social Security Number

The following Federal laws establish a framework for restricting Social Security number (SSN) disclosure.[1]

The Freedom of Information Act of 1966 (5 U.S.C. 552)

The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of Executive Branch agencies and departments are accessible to the people. FOIA, as amended, provides that the public has a right of access to Federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the Government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to State and local governments.

The Privacy Act of 1974 (5 U.S.C. 552a)

The Privacy Act regulates Federal agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records. The Act prohibits the disclosure of any record contained in a system of records unless the disclosure is made based on a written request or prior written consent of the person to whom the records pertain or is otherwise authorized by law. The Act authorizes 12 exceptions under which an agency may disclose information in its records.

The Act contains a number of additional provisions that restrict Federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or Executive Order of the President, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under Federal programs.

[1] Summarized from *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii))[2]

The Social Security Act bars disclosure by Federal, State and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the Act also contains criminal penalties for "unauthorized willful disclosures" of SSNs. Because the Act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by Federal entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear whether the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to Federal, State and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

[2] Pub. L. No. 101-624 §2201, 104 Stat. 3359, 3951 (1990).

Appendix B

Participating Offices of Inspector General

Department of Agriculture

Department of Defense

Department of Education

Department of Health and Human Services

Department of Housing and Urban Development

Department of Labor

Department of the Treasury

Environmental Protection Agency

Federal Deposit Insurance Corporation

Nuclear Regulatory Commission

Office of Personnel Management

Railroad Retirement Board

Small Business Administration

Social Security Administration

Treasury Inspector General for Tax Administration

Summary of Inadequate Controls Identified by Offices of Inspector General (OIG)

Federal Agency and Program(s) Reviewed	INADEQUATE CONTROLS IDENTIFIED BY OIGs			
	Contractor Access and Use of SSNs	Access to SSNs Maintained in Agency Databases	Non-Government/ Non-contractor Access and Use of SSNs	Legal and Informed Disclosure of SSNs to External Entities
Department of Agriculture: Food Stamp Program	X[1]	X[1]		
Department of Defense: Defense Manpower Data Center; Army and Air Force Exchange Service, and Defense Security Service	X[2]	X[3]		
Department of Education: Pell Grant Program	X	X		
Department of Health and Human Services: Food and Drug Administration	X			X
Department of Housing and Urban Development: Office of Housing	X			

[1] Inadequate controls identified at the State/local levels of the Food Stamp Program.

[2] Inadequate controls over contractor access and use of SSNs identified in the following Department of Defense agencies: Army and Air Force Exchange Service and Defense Security Service.

[3] Inadequate controls over access to SSNs maintained in its databases identified at the Defense Manpower Data Center.

Federal Agency and Program(s) Reviewed	Inadequate Controls Identified by OIGs			
	Contractor Access and Use of SSNs	Access to SSNs Maintained in Agency Databases	Non-Government/ Non-contractor Access and Use of SSNs	Legal and Informed Disclosure of SSNs to External Entities
Department of Labor: Federal Employee Compensation Act Program	X		X	
Department of the Treasury: Financial Management Service	X	X		
Environmental Protection Agency: Financial Management and Financial Services Divisions				
Federal Deposit Insurance Corporation	X		X	
Nuclear Regulatory Commission	X	X		
Office of Personnel Management: Retirement and Insurance Service, Office of Merit Systems Oversight and Effectiveness, and Investigations Service	X	X		
Railroad Retirement Board	X	X		
Small Business Administration	X			
Social Security Administration: Title II Program	X	X		
Treasury Inspector General for Tax Administration: Internal Revenue Service	X	X		
TOTALS	**14**	**9**	**2**	**1**